File DVD 2000

CONFIDENTIAL

MPA BRIEFING NOTE ON THE DVD HACK (DeCSS) FOR THE RIGHTSHOLDERS COALITION

THE DVD AND CSS:

The introduction of the DVD was delayed for several years because the audio-visual industry recognised the danger of introducing a new digital format that could be a template for the creation and distribution of unlimited, perfect copies. As a result, the MPA member companies did not agree to make their content available for distribution on DVDs until technical protection was developed to protect it. This position led to the development of the CSS (Content Scrambling System) encryption technology by Matsushita Electric Industrial Company Limited (MEI). In essence, the CSS is a scrambling system designed to make the copying of a DVD impossible. All manufacturers of DVD hardware use this system under a license granted by the DVD Copy Control Association (CCA).

THE CSS PROTECTION SYSTEM:

CSS is an encryption-based security and authentication system that requires the use of appropriately-configured hardware (e.g., a DVD player or computer DVD drive) to decrypt, unscramble and play back copies of motion pictures on DVDs. The content of the DVD is stored in a scrambled form designed to prevent copying. In order to view the film the picture must be unscrambled. To do so, the CSS needs a "key", which in effect unlocks the code. In PCs, the actual unscrambling is performed by a number of commercially available computer programs such as WinDVD, ATI DVD or XING DVD. The key is actually stored on the DVD itself but it is hidden in a secret sector. The DVD will only allow this key to be read if it is accessed by an algorithm, which was designed by MEI, and is the industry standard. In hardware devices such as a DVD player it is contained within a larger program stored on a microprocessor. On computers, it is contained within a larger program stored on the computer's hard disc. The algorithm actually provides the key. The larger program, which surrounds the algorithm, provides security devices designed to prevent access to the algorithm. These devices include encrypting the algorithm itself and a utility that causes the computer to crash if the algorithm is accessed.

THE HACK - DeCSS:

On or about October 25, 1999, an individual or group of individuals in Europe managed to hack the DVD encryption system and began to offer, via the Internet, a software utility called DeCSS that enables users to effectively "break" the CSS copy protection system and thereby make and distribute digital copies of DVD movies. DeCSS functions by emulating the genuine CSS algorithm, which is a computer program that produces a "result" (i.e., it allows the "key" to be read). In other words, it allows a non-CSS-compliant DVD player to play, store, copy, or transmit digital copies of DVD content. DeCSS breaks the CSS encryption. DeCSS differs from "DVD Rippers" which only allow analogue copies of DVDs to be made but do not break the encryption. DeCSS can

be used, therefore, to create legitimate-quality DVDs. While it is possible that the "hack" occurred as a result of a completely new program, it is more likely that the hackers accessed the genuine algorithm and have copied those parts which produce the "result". It was reported in the press that DVD software produced by Xing Technologies, a Japanese company which has recently been acquired by Real Networks, had been marketed without protection, in the sense that a program used to protect the algorithm had not been included within the device. Thus, it is believed that the hackers were able to copy the algorithm contributing to the development of DeCSS.

DVD CCA ACTION:

The CCA complaint seeking a temporary restraining order (TRO is a form of interim relief), which was filed in a California court in December, asserts that the person who created DeCSS must have accepted and then violated the terms of the "click wrap" license. All manufacturers of DVD hardware use the CSS under a license granted by DVD Copy Control Association (CCA). This license includes a provision that requires CCA to enjoin public disclosure of the trade secrets embodied in CSS. Xing in turn requires Xing software users to agree to the terms of a "click wrap" license that prohibits reverse engineering. The CCA's efforts to secure a TRO against 72 named and unknown defendants to prohibit the further use or disclosure of DeCSS were unsuccessful. The judge did not give reasons for his refusal to grant a TRO. The same judge considered CCA's application for a preliminary injunction on 18 January. He will likely give his decision in a few days. The CCA argued that CSS was reverse engineered in violation of the CSS and Xing licenses and that as the trade secrets embodied in CSS were obtained improperly, the defendants should be enjoined from using or disclosing them. The defendants argued that CSS was too weak to protect the trade secrets and that reverse engineering was in any case lawful in Norway (where it is believed CSS was first hacked). They also argued that the CCA was seeking to prevent the defendants from engaging in academic research and from exercising their constitutional right to free speech, and that, once posted on the Internet, a trade secret loses its protection.

Many people in the Internet community have rejected the proposition that it was necessary to breach the Xing license in order to create DeCSS, arguing that no one knows who created DeCSS, or how. CCA must prove that there was a violation of a contractual duty to protect the CSS trade secrets in order to prohibit either reverse engineering CSS or "engineering around" the CSS encryption under California trade secret law. They have also raised reverse-engineering (to achieve Linux compatibility) arguments. As noted above, the judge has not yet addressed the merits of the case.

MPA ACTIONS:

The MPA first became aware of DeCSS on 25 October 1999. It was traced back to a website owned by Jon Johansen in Norway. However, since its first appearance, DeCSS has been posted on, or linked-to, thousands of websites around the world, and is probably in the possession of thousands of individuals. The MPA has sent out cease-and-desist

notices to over 185 websites, but less than 1/3 of these have complied. Given the fact that hackers take pride in collecting and distributing films regardless of the cost or effort involved, the MPA expects to see DVD datafiles circulating within hacker groups in the near future.

The MPA Member Companies filed federal actions on 14 January in New York and Connecticut seeking interim relief under the anti-circumvention provisions of the Digital Millennium Copyright Act (DMCA), against a number of distributors of DeCSS. The claims are for injunctive relief and for money damages and related relief against some of those responsible for proliferating DeCSS so that individuals can make, distribute, and/or otherwise electronically transmit or perform unauthorized copies of the MPA Member Companies' copyrighted motion pictures and other audio-visual works. On Thursday, January 20, New York Federal Judge Lewis A. Kaplan granted the request for a preliminary injunction against three New York-based defendants. They must immediately remove DeCSS from their Web sites. The result is a major victory in the battle against digital piracy.

With respect to "anti-circumvention devices", the DMCA provides that

> "No person shall ... offer to the public, provide, or otherwise traffic in any technology, product, service, device, [or] component... that is primarily designed or produced for the purpose of circumventing protection afforded by a technological measure that effectively controls access to a copyrighted work or protects a right of a copyright owner...."

The language "circumventing protection" means avoiding, bypassing, removing, deactivating, or otherwise impairing a technological measure. A "technological measure...prevents, restricts, or otherwise limits the exercise of a right of a copyright owner." The CSS is a technological measure because it limits people with DVDs from making unauthorised copies. Any person injured by a violation of the anti-circumvention rules above may bring a civil action in an appropriate US District court. The injury will result from the eventual theft of intellectual property contained in the DVDs. The court may also award damages, costs, and fees.

THE PUBLIC PERCEPTION OF THE DVD HACK

The DVD hack has raised several first amendment (freedom of speech) and reverse-engineering issues. The implication is that the film industry is somehow seeking to stifle free speech. The purpose of the CSS is to protect copyright works. This is an important public policy recognised by the US Constitution, other national laws and international law. Moreover, the DMCA, which provides legal protection for technical measures in fulfilment of international obligations under the WIPO Copyright Treaties, foresees the development of such measures. The circumvention of these measures protected by such legislation is a crime. The issue of free speech is not relevant. With respect to the DMCA, there is no conflict with free speech because the DMCA does not prevent fair use. Fair

use does not extend to the copying of entire works. There is scope for research and reverse engineering under the DMCA subject to certain limitations. These exceptions were not however intended to permit the dissemination of circumvention devices, which are designed to infringe the DMCA anti-circumvention provisions as well as other laws. It is clear from the press and on-line chat forums that the real goals of those now involved in disseminating the DeCSS is not to exercise their freedom of expression but the desire to damage the film industry. The resultant damage threatens the future production of audio-visual works, thereby causing injury to film producers, directors, actors, distributors, exhibitors and the many other people involved in the production and distribution of films, not only in the US, but world-wide.

THE PROPOSED EU COPYRIGHT DIRECTIVE:

In confronting this issue and due to the international nature of the Internet, the legislative situation in the EU is obviously important, particularly due to the fact that the "hack" appears to have occurred in Europe. These events highlight the importance of the effective implementation of the WIPO Copyright Treaties. In the EU, the Proposed Copyright Directive, which is meant to implement these treaties, also contains legal protection for technical measures.

In order to address the DVD hack (and other forms of illicit circumvention), rightsholders need a strong Copyright Directive backed up by effective enforcement. The Copyright Directive, which is currently being debated by the Member States (in the Council Working Group), should be adopted quickly but not at the expense of effective protection. To the extent that rightsholders are unable to enforce the legal protection for technical measures in the Copyright Directive because it sanctions non-infringing uses, we will be severely limited in our ability to address problems like DeCSS. In the digital environment, rightsholders will use technical measures to ensure the delivery of an ever-wider range of copyright materials. The traditional notions of private copying are not relevant. The DVD is a robust medium. Therefore, the argument that individuals need to make back-up (private) copies of DVDs does not hold water. The only reason for making such copies would be for further distribution, which risks severely damaging the audio-visual sector. The existence of exceptions that are not subordinate to technical measures would render such measures useless. The result would be to negate the purpose of the Copyright Directive and the WIPO Copyright Treaties and to destroy rightsholders' ability to distribute their works in the digital environment.

It should also be noted that a blanket exception for temporary copies (Article 5.1) which eliminates any incentives for service providers to co-operate in the fight against piracy will further exacerbate the challenges posed by the spread of illicit circumvention devices which enable the unauthorised distribution of DVDs on the Internet. The limitations on liability in the E-Commerce Directive (which has recently been the subject of a political agreement by the Member States) provide a workable means for protecting the interests